

## CLAIMS

That which is claimed:

1. A method of operating a communication network, comprising:  
detecting an anomaly in communication traffic at a plurality of nodes in the communication network;  
independently applying at respective ones of the plurality of nodes a first  
5 blocking measure A to the anomalous traffic that stops the anomalous traffic; and  
independently determining at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.  
10
2. The method of Claim 1, wherein independently determining the second blocking measure B comprises:  
applying a logical combination of A and a second blocking measure B given by (A & !B) to the anomalous traffic, wherein the logical combination (A & !B) is a  
15 less restrictive blocking measure than a logical combination (A & B); and  
enforcing the logical combination (A & !B) if the logical combination (A & !B) stops the anomalous traffic.
3. The method of Claim 2, further comprising:  
20 independently determining a third blocking measure C at the respective ones of the plurality of nodes such that application of a logical combination of (A & !B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & !B) stops the anomalous traffic.
- 25 4. The method of Claim 2, wherein independently determining the second blocking measure B further comprises:  
applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and  
enforcing the logical combination (A & B) if the logical combination (A & B)  
30 stops the anomalous traffic.

5. The method of Claim 4, further comprising:

independently determining a third blocking measure C at the respective ones  
of the plurality of nodes such that application of a logical combination of (A & B) and  
5 the third blocking measure C to the anomalous traffic stops the anomalous traffic if  
the logical combination (A & B) stops the anomalous traffic.

6. The method of Claim 4, further comprising:

determining a third blocking measure C at the respective ones of the plurality  
10 of nodes such that application of a logical combination of A and the third blocking  
measure C to the anomalous traffic stops the anomalous traffic if the logical  
combination (A & B) does not stop the anomalous traffic.

7. The method of Claim 1, wherein detecting an anomaly in the

15 communication traffic comprises:

comparing the communication traffic to at least one anomaly factor; and  
detecting the anomaly in the communication traffic at the plurality of nodes in  
the communication network if the at least one anomaly factor is present in the  
communication traffic.

20

8. The method of Claim 1, further comprising:

assigning a severity to the detected anomaly; and  
wherein independently applying the first blocking measure A to the anomalous  
traffic comprises independently applying the first blocking measure A to the  
25 anomalous traffic at each of the plurality of nodes in the communication network that  
stops or reduces the flow of the anomalous traffic based on the severity of the detected  
anomaly.

9. The method of Claim 1, further comprising:

30 intentionally inserting the anomaly in the communication traffic; and  
associating the first blocking measure A and the second blocking measure B  
with the anomaly.

10. A method of operating a communication network, comprising:  
detecting an anomaly in communication traffic at a plurality of nodes in the  
communication network;

5 synchronously applying at respective ones of the plurality of nodes a first  
blocking measure A to the anomalous traffic that stops the anomalous traffic; and  
synchronously determining at the respective ones of the plurality of nodes a  
second blocking measure B such that application of a logical combination of the first  
blocking measure A and the second blocking measure B to the anomalous traffic stops  
the anomalous traffic.

10

11. A system for operating a communication network, comprising:  
means for detecting an anomaly in communication traffic at a plurality of  
nodes in the communication network;

15 means for independently applying at respective ones of the plurality of nodes a  
first blocking measure A to the anomalous traffic that stops the anomalous traffic; and  
means for independently determining at the respective ones of the plurality of  
nodes a second blocking measure B such that application of a logical combination of  
the first blocking measure A and the second blocking measure B to the anomalous  
traffic stops the anomalous traffic.

20

12. The system of Claim 11, wherein the means for independently  
determining the second blocking measure B comprises:

25 means for applying a logical combination of A and a second blocking measure  
B given by  $(A \ \& \ !B)$  to the anomalous traffic, wherein the logical combination  $(A \ \& \ !B)$   
is a less restrictive blocking measure than a logical combination  $(A \ \& \ B)$ ; and  
means for enforcing the logical combination  $(A \ \& \ !B)$  if the logical  
combination  $(A \ \& \ !B)$  stops the anomalous traffic.

13. The system of Claim 12, further comprising:  
30 means for independently determining at the respective ones of the plurality of  
nodes a third blocking measure C such that application of a logical combination of  $(A \ \& \ !B)$   
and the third blocking measure C to the anomalous traffic stops the anomalous  
traffic if the logical combination  $(A \ \& \ !B)$  stops the anomalous traffic.

14. The system of Claim 12, wherein the means for independently determining the second blocking measure B further comprises:

- 5 means for applying a logical combination (A & B) to the anomalous traffic if the logical combination (A & !B) does not stop the anomalous traffic; and  
means for enforcing the logical combination (A & B) if the logical combination (A & B) stops the anomalous traffic.

15. The system of Claim 14, further comprising:  
10 means for independently determining at the respective ones of the plurality of nodes a third blocking measure C such that application of a logical combination of (A & B) and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) stops the anomalous traffic.

- 15 16. The system of Claim 14, further comprising:  
means for determining at the respective ones of the plurality of nodes a third blocking measure C such that application of a logical combination of A and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination (A & B) does not stop the anomalous traffic.

- 20 17. The system of Claim 11, wherein the means for detecting an anomaly in the communication traffic comprises:  
means for comparing the communication traffic to at least one anomaly factor;  
and  
25 means for detecting the anomaly in the communication traffic at the plurality of nodes in the communication network if the at least one anomaly factor is present in the communication traffic.

18. The system of Claim 11, further comprising:  
30 means for assigning a severity to the detected anomaly; and  
wherein the means for independently applying the first blocking measure A to the anomalous traffic comprises means for independently applying the first blocking measure A to the anomalous traffic at each of the plurality of nodes in the

communication network that stops or reduces the flow of the anomalous traffic based on the severity of the detected anomaly.

19. The system of Claim 11, further comprising:  
5 means for intentionally inserting the anomaly in the communication traffic;  
and  
means for associating the first blocking measure A and the second blocking measure B with the anomaly.

10 20. A system for operating a communication network, comprising:  
means for detecting an anomaly in communication traffic at a plurality of nodes in the communication network;  
means for synchronously applying at respective ones of the plurality of nodes a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and  
15 means for synchronously determining a second blocking measure B at the respective ones of the plurality of nodes such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.

20 21. A computer program product for operating a communication network, comprising:  
a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:  
computer readable program code configured to detect an anomaly in  
25 communication traffic at a plurality of nodes in the communication network;  
computer readable program code configured to independently apply at respective ones of the plurality of nodes a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and  
computer readable program code configured to independently determine at the  
30 respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.

22. The computer program product of Claim 21, wherein the computer readable program code configured to independently determine the second blocking measure B comprises:

5 computer readable program code configured to apply a logical combination of A and a second blocking measure B given by  $(A \ \& \ !B)$  to the anomalous traffic, wherein the logical combination  $(A \ \& \ !B)$  is a less restrictive blocking measure than a logical combination  $(A \ \& \ B)$ ; and

10 computer readable program code configured to enforce the logical combination  $(A \ \& \ !B)$  if the logical combination  $(A \ \& \ !B)$  stops the anomalous traffic.

23. The computer program product of Claim 22, further comprising:

15 computer readable program code configured to independently determine at the respective ones of the plurality of nodes a third blocking measure C such that application of a logical combination of  $(A \ \& \ !B)$  and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination  $(A \ \& \ !B)$  stops the anomalous traffic.

24. The computer program product of Claim 22, wherein the computer readable program code configured to independently determine the second blocking measure B further comprises:

20 computer readable program code configured to apply a logical combination  $(A \ \& \ B)$  to the anomalous traffic if the logical combination  $(A \ \& \ !B)$  does not stop the anomalous traffic; and

25 computer readable program code configured to enforce the logical combination  $(A \ \& \ B)$  if the logical combination  $(A \ \& \ B)$  stops the anomalous traffic.

25. The computer program product of Claim 24, further comprising:

30 computer readable program code configured to independently determine at the respective ones of the plurality of nodes a third blocking measure C such that application of a logical combination of  $(A \ \& \ B)$  and the third blocking measure C to the anomalous traffic stops the anomalous traffic if the logical combination  $(A \ \& \ B)$  stops the anomalous traffic.

26. The computer program product of Claim 24, further comprising:  
computer readable program code configured to determine at the respective  
ones of the plurality of nodes a third blocking measure C such that application of a  
logical combination of A and the third blocking measure C to the anomalous traffic  
5 stops the anomalous traffic if the logical combination (A & B) does not stop the  
anomalous traffic.

27. The computer program product of Claim 21, wherein the computer  
readable program code configured to detect an anomaly in the communication traffic  
10 comprises:  
computer readable program code configured to compare the communication  
traffic to at least one anomaly factor; and  
computer readable program code configured to detect the anomaly in the  
communication traffic at the plurality of nodes in the communication network if the at  
15 least one anomaly factor is present in the communication traffic.

28. The computer program product of Claim 21, further comprising:  
computer readable program code configured to assign a severity to the detected  
anomaly; and  
20 wherein the computer readable program code configured to independently  
apply the first blocking measure A to the anomalous traffic comprises computer  
readable program code configured to independently apply the first blocking measure  
A to the anomalous traffic at each of the plurality of nodes in the communication  
network that stops or reduces the flow of the anomalous traffic based on the severity  
25 of the detected anomaly.

29. The computer program product of Claim 21, further comprising:  
computer readable program code configured to intentionally insert the anomaly  
in the communication traffic; and  
30 computer readable program code configured to associate the first blocking  
measure A and the second blocking measure B with the anomaly.

30. A computer program product for operating a communication network, comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

5 computer readable program code configured to detect an anomaly in communication traffic at a plurality of nodes in the communication network;

computer readable program code configured to synchronously apply at respective ones of the plurality of nodes a first blocking measure A to the anomalous traffic that stops the anomalous traffic; and

10 computer readable program code configured to synchronously determine at the respective ones of the plurality of nodes a second blocking measure B such that application of a logical combination of the first blocking measure A and the second blocking measure B to the anomalous traffic stops the anomalous traffic.